UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/748,845	12/29/2003	Jeremey Barrett	59864.00876	2762

32294 7590 07/06/2009
SQUIRE, SANDERS & DEMPSEY L.L.P.
8000 TOWERS CRESCENT DRIVE
14TH FLOOR
VIENNA, VA 22182-6212

EXAMINER	
BHATIA, AJAY M	
ART UNIT	PAPER NUMBER
2445	
MAIL DATE	DELIVERY MODE
07/06/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

____

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

____

Ex parte JEREMEY BARRETT, CRAIG R. WATKINS,
and ADAM CAIN

____

Appeal 2008-005229
Application 10/748,845
Technology Center 2400

____

Decided:[1] July 6, 2009

____

Before JAMES D. THOMAS, JOHN A. JEFFERY, and THU A. DANG, *Administrative Patent Judges.*

JEFFERY, *Administrative Patent Judge.*

DECISION ON APPEAL

[1] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, begins to run from the decided date shown on this page of the decision. The time period does not run from the Mail Date (paper delivery) or Notification Date (electronic delivery).

Appellants appeal under 35 U.S.C. § 134(a) from the Examiner's rejection of claims 1-28. We have jurisdiction under 35 U.S.C. § 6(b). We affirm.

STATEMENT OF THE CASE

Appellants invented a system for managing a proxy request over a secure network using inherited security attributes. A secure tunnel service receives a proxy request from a client and modifies the proxy request to include a security attribute. The modified proxy request is then forwarded to a proxy service where the security attribute enables a proxy connection through the secure tunnel.[2] Claim 1 is illustrative:

> 1. A network device for managing a communication over a network, comprising:
>
> a transceiver configured to send and to receive the communication over the network;
>
> a processor, coupled to the transceiver, that is configured to:
>
> receive a proxy request from a client through a secure tunnel;
>
> modify the proxy request to include a security attribute inherent from the secure tunnel; and
>
> forward the modified proxy request to a proxy service,
>
> wherein the security attribute enables a proxy connection through the secure tunnel.

[2] *See generally* Abstract; Spec. 15-16.

The Examiner relies on the following as evidence of unpatentability:

Spacey	US 2002/0038371 A1	Mar. 28, 2002

The Examiner rejected claims 1-28 under 35 U.S.C. § 102(b) as anticipated by Spacey. Ans. 3-5.

Rather than repeat the arguments of Appellants or the Examiner, we refer to the Briefs and the Answer[3] for their respective details. In this decision, we have considered only those arguments actually made by Appellants. Arguments which Appellants could have made but did not make in the Briefs have not been considered and are deemed to be waived. *See* 37 C.F.R. § 41.37(c)(1)(vii).

Regarding representative claim 1,[4] the Examiner finds that Spacey teaches all of the claimed subject matter including a secure Virtual Private Network (VPN) tunnel. According to the Examiner, Spacey in Figure 7 teaches a processor that (1) receives a proxy request through the secure tunnel; (2) modifies the proxy request to include a security attribute inherent from the secure tunnel via the SSL-based communications; and (3) forwards the request to a proxy service (proxy client) to enable a proxy connection through the secure tunnel. Ans. 3, 5-6.

[3] Throughout this opinion, we refer to (1) the Appeal Brief filed February 6, 2008; (2) the Examiner's Answer mailed April 2, 2008; and (3) the Reply Brief filed June 2, 2008.

[4] Although Appellants nominally argue claims 2-6 separately from claim 1 (App. Br. 9-10), Appellants present no distinct substantive arguments regarding these dependent claims. Accordingly, we group claims 1-6 together and select claim 1 as representative. *See* 37 C.F.R. § 41.37(c)(1)(vii).

Appellants argue that Spacey does not disclose a processor that modifies the proxy request to include a security attribute inherent from the secure tunnel, and forward the modified proxy request to a proxy service as claimed. According to Appellants, Spacey merely teaches an intermediary server of a VPN that (1) verifies registration requests of two proxy clients using an SSL communication channel, and (2) holds open the proxy client connection for passing client requests therethrough. Appellants emphasize that Spacey's system does not modify the two proxy clients' requests, let alone include a security attribute inherent from the secure tunnel as claimed. App. Br. 6-9; Reply Br. 3-7.

The issue before us, then, is as follows:

ISSUE

Under § 102, have Appellants shown that the Examiner erred in rejecting claim 1 by finding that Spacey discloses a processor that (1) receives a proxy request through a secure tunnel; (2) modifies the proxy request to include a security attribute inherent from the secure tunnel; and (3) forwards the request to a proxy service to enable a proxy connection through the secure tunnel as claimed?

FINDINGS OF FACT

The record supports the following findings of fact (FF) by a preponderance of the evidence:

Spacey

1. Spacey discloses a system for providing services over a communication channel or network through an intermediary apparatus. In

one implementation, a VPN can be constructed through two networks and/or machines through the intermediary. Spacey, ¶¶ 0001, 0016-17.

2. One implementation of Spacey's system enables communication between two distinct private networks via an intermediary server as shown in Figure 7. To this end, network datagrams destined for a computer on the opposite network are (1) sent to the modified routers; (2) encapsulated with virtual address information; (3) sent to the intermediary; and (4) passed to the appropriate destination proxy client for repeating at the network layer on the destination network. Spacey, ¶¶ 0119-21; Fig. 7.

3. Initially, both networks' proxy clients register their virtual addresses with the intermediary server by (1) opening an outbound Secure Sockets Layer (SSL) communication channel with the intermediary using the SSL protocol, and (2) sending a registration request to the intermediary through their SSL channels. Spacey, ¶¶ 0122-24; Fig. 7.

4. Upon verifying the proxy clients' registration, the intermediary holds open the proxy client connection such that it is ready to pass client requests therethrough. With both proxy clients connected to the intermediary, communication can pass through the restrictive firewalls unhindered. Spacey, ¶¶ 0125-27.

5. Then, if user (Fred Smith) on the satellite network sends an email destined for the opposite network, the associated datagram is routed through the local modified router. The modified router adds a virtual address header and sends the datagram to the intermediary to identify the correct proxy client to which to forward the datagram. The modified router also (1) opens an SSL communications channel through the firewall to the intermediary; (2) provides authentication data (username, password, and destination

combination); and (3) sends the datagram through the open SSL connection as a stream. Spacey, ¶¶ 0131-35; Figs. 7 and 8.

6. Upon receipt, the intermediary identifies the destination proxy client, and verifies that the modified router is allowed to communicate with this proxy client. If so, the intermediary (1) waits to receive the network datagram encapsulated in the SSL communication channel stream, and (2) forwards it to the waiting proxy client on the destination network. Spacey, ¶ 0137; Figs. 7 and 8.

7. Spacey's Figure 9 indicates that after the intermediary interprets the request header to identify the correct proxy client connection, the intermediary drops the modifier router header and waits for the encapsulated datagram to be sent to the opposite network. Spacey, Fig. 9 ("Intermediary" column).

Appellants' Disclosure

8. According to Appellants' Specification, a secure tunnel includes "virtually any mechanism that enables a secure communication over a network between a client and a server." The Specification further notes that a secure tunnel can include SSL. Spec. 10:1-9.

9. Appellants' Specification notes that "[t]he security attribute may be associated with a property of a secure tunnel . . . [and] may also be associated with a security property of a client . . . . Such security properties may include access control data, IP address, digital certificate, and the like." Spec. 11:6-11.

10. The Specification also notes that the security attribute may further include, but is not limited to, a security credential associated with the client,

a session identifier, a cipher setting, randomly generated data, an encrypted password, etc. According to Specification, the security attribute may include "virtually any security attribute associated with the secure tunnel" and can modify a packet header, encapsulation header, and the like. Spec. 16:5-22.

PRINCIPLES OF LAW

Anticipation is established only when a single prior art reference discloses, expressly or under the principles of inherency, each and every element of a claimed invention as well as disclosing structure which is capable of performing the recited functional limitations. *RCA Corp. v. Appl. Dig. Data Sys., Inc.*, 730 F.2d 1440, 1444 (Fed. Cir. 1984); *W.L. Gore & Assoc., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1554 (Fed. Cir. 1983).

"'[T]eaching away' is irrelevant to anticipation." *Leggett & Platt, Inc. v. VUTEk, Inc.*, 537 F.3d 1349, 1356 (Fed. Cir. 2008) (citation omitted).

ANALYSIS

Claims 1-6

Based on the record before us, we find no error in the Examiner's anticipation rejection of representative claim 1. Claim 1 calls for, in pertinent part, a processor that (1) receives a proxy request through a secure tunnel; (2) modifies the proxy request to include a security attribute inherent from the secure tunnel; and (3) forwards the request to a proxy service to enable a proxy connection through the secure tunnel.

Turning to Spacey, we find—as did the Examiner (Ans. 5 and 6)—that Spacey's VPN capabilities that securely communicate data over SSL communications channels (*see* FF 1-7) fully meet a "secure tunnel" as claimed. Indeed, this finding fully comports with Appellants' own description of the term in the Specification. *See* FF 8.

We also find that requests sent through this secure tunnel are modified to include security attributes inherent from the secure tunnel as claimed. Appellants are correct (Reply Br. 6-7) that the two proxy clients' initial requests to the intermediary are not modified, but rather enable the intermediary to hold open connections to those proxy clients for subsequent communications through those connections. *See* FF 3 and 4.

But nothing in the claim precludes the recited client "proxy request" from corresponding to the datagram in Spacey that is sent to the opposite network via the modified router and the intermediary. *See* FF 5 and 6. In particular, nothing in the claim precludes the intermediary's receipt of a "proxy request" through the secure tunnel between the modified router and the intermediary (i.e., the SSL channel between the router and the intermediary). *See id.*

Nor does the claim preclude the intermediary in Spacey from modifying that received request to include a security attribute inherent from the tunnel. After the intermediary receives communication from the modified router, it (1) interprets the request header to identify the appropriate destination proxy client; (2) drops the modifier router header; and (3) sends the encapsulated datagram to the opposite network. FF 6 and 7. As such, the intermediary not only modifies the received request, but also includes a security attribute inherent from the secure tunnel—namely the SSL security features inherent from the SSL secure tunnel through which the encapsulated datagram was sent. *See* FF 5-7.

Lastly, we find unavailing Appellants' contention that Spacey's use of an intermediary teaches away from an L2TP encapsulation (App. Br. 8), for "teaching away" arguments are irrelevant to anticipation rejections. *See Leggett & Platt*, 537 F.3d at 1356.

For the foregoing reasons, Appellants have not persuaded us of error in the Examiner's rejection of representative claim 1. Therefore, we will sustain the Examiner's rejection of that claim, and claims 2-6 which fall with claim 1.

Claims 7-28

We will also sustain the Examiner's anticipation rejection of claims 7-28. Although Appellants present separate arguments for independent claims 7, 10, 18, and 27 and nominally argue their respective dependent claims (App. Br. 10-26), Appellants essentially reiterate the same arguments presented for independent claim 1 and provide no distinct substantive basis for separate patentability of the dependent claims. Since we are not persuaded by these arguments, we will sustain the Examiner's rejection of claims 7-28 for the same reasons as indicated above with respect to claim 1.[5]

[5] We note in passing that claim 10 is broader than the other independent claims in a significant respect, namely that security attribute does not have to be inherent from the secure tunnel. As such, Appellants' arguments pertaining to this limitation (*see, e.g.*, App. Br. 15; *see also* Reply Br. 7) are not commensurate with the scope of claim 10. Nevertheless, even if claim 10 did recite this feature, we find the limitation fully met by Spacey as indicated previously.

CONCLUSION

Appellants have not shown that the Examiner erred in rejecting claims 1-28 under § 102.

DECISION

The Examiner's decision rejecting claims 1-28 is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

msc

SQUIRE, SANDERS & DEMPSEY L.L.P.
8000 TOWERS CRESCENT DRIVE
14TH FLOOR
VIENNA VA 22182-6212